1. A device for secure computing, comprising:

a) a computer system, where the computer system includes a processor;

b) an operating-system software-program loaded onto the processor of the computer system;

c) a type-II virtual-machine monitor software-program loaded onto the operating-system software-program of the computer system;

d) a user-definable number of non-sensitive virtual-machines;

e) a user-definable number of sensitive virtual-machines, where each sensitive virtual-machine has a user-definable sensitivity level;

f) a user-definable number of encryption virtual-machines, where each encryption virtual-machine is connected to one of said user-definable number of sensitive virtual-machines, and where each encryption virtual-machine includes at least one encryption algorithm capable of encrypting information from the corresponding sensitive virtual-machine according to the corresponding sensitivity level; and

g) a router virtual-machine connected to each non-sensitive virtual-machine and each encryption virtual-machine.

2. The device of claim 1, wherein said operating-system software program is selected from the group of operating-system software programs consisting of Windows 2000, Windows NT, Linux, and any other suitable operating-system software program.

3. The device of claim 1, wherein each of said encryption virtual-machines outputs information according to Internet Protocol Security standards.

4. The device of claim 1, wherein each of said encryption virtual-machine includes at least one encryption algorithm selected from the group of encryption algorithms consisting of an encryption algorithm, a key exchange algorithm, a digital signature algorithm, and any combination thereof.

5. The device of claim 1, further comprising a server connected to each non-sensitive virtual-machine and each sensitive virtual-machine.

6. The device of claim 5, wherein said server is selected from the group of servers consisting of a stand-alone device and a virtual machine.

7. The device of claim 1, further comprising a checker connected to each of said encryption virtual-machines and to the router virtual-machine.

8. The device of claim 7, wherein said checker is selected from the group of checkers consisting of a stand-alone device and a virtual machine.

9. A method of secure computing, comprising the steps of:

a) acquiring a computer system, where the computer system includes a processor;

b) loading a host operating-system software program onto the processor of the computer system;

c) loading a type-II virtual machine monitor software program onto the operating system of the computer system;

d) creating a user-definable number of non-sensitive virtual-machines;

e) creating a user-definable number of sensitive virtual-machines, where each sensitive virtual-machine has a user-definable sensitivity level;

f) creating a user-definable number of encryption virtual-machines, where each encryption virtual-machine is connected to one of said user-definable number of sensitive virtual-machines, and where each encryption virtual-machine includes at least one encryption algorithm capable of encrypting information from the corresponding sensitive virtual-machine according to the corresponding sensitivity level; and

g) creating a router virtual-machine connected to each non-sensitive virtual-machine and each encryption virtual-machine.

10. The method of claim 9, wherein said step of loading a host operating-system software-program is comprised of the step of loading an operating-system software program selected from the group of operating-system software programs consisting of Windows 2000, Windows NT, Linux, and any other suitable operating system.

11. The method of claim 9, wherein said step of creating a user-definable number of encryption virtual-machines is comprised of the step of creating a user-definable number of encryption virtual-machines that each outputs information according to an Internet Protocol Security standard.

12. The method of claim 9, wherein said step of creating a user-definable number of encryption virtual-machines is comprised of the step of creating a user-definable number of encryption

virtual-machines wherein each encryption virtual-machine includes at least one encryption algorithm selected from the group of encryption algorithms consisting of an encryption algorithm, a key exchange algorithm, a digital signature algorithm, and any combination thereof.

13. The method of claim 9, further comprising the step of transferring information between each of said non-sensitive virtual-machine and sensitive virtual-machine when appropriate.

14. The method of claim 9, further comprising the step of checking to see that each encryption virtual-machine is operating properly and, if not, disconnecting the router virtual-machine from a network.